



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728
7590	08/29/2005		EXAMINER	
WAGNER, MURABITO & HAO LLP			LANIER, BENJAMIN E	
Third Floor			ART UNIT	PAPER NUMBER
Two North Market Street				
San Jose, CA 95113			2132	

DATE MAILED: 08/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/972,371	IWAMURA, RYUICHI	
	Examiner Benjamin E. Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on ____.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-25 is/are pending in the application.
 - 4a) Of the above claim(s) 8-16 and 21-25 is/are withdrawn from consideration.
- 5) Claim(s) ____ is/are allowed.
- 6) Claim(s) 1-7 and 17-20 is/are rejected.
- 7) Claim(s) ____ is/are objected to.
- 8) Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 05 October 2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. ____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: ____.
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date: ____.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: ____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-7, 17-20, drawn to a method of securely processing a digital signal between two parties, classified in class 713, subclass 189.
 - II. Claims 8-16, drawn to a method of securely processing a digital signal between three parties, classified in class 713, subclass 155.
 - III. Claims 21-25, drawn to a method for modifying an encryption technique, classified in class 713, subclass 170.
2. The inventions are distinct, each from the other because of the following reasons:

Inventions I-III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such of content distribution between two parties. See MPEP § 806.05(d). In the instant case, invention II has separate utility such of content distribution between three parties. See MPEP § 806.05(d). In the instant case, invention III has separate utility such of modifying encryption techniques. See MPEP § 806.05(d).
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II and III, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and the search required for Group II is not required for Group I and III, restriction for examination purposes as indicated is proper.

6. Because these inventions are distinct for the reasons given above and the search required for Group III is not required for Group I and II, restriction for examination purposes as indicated is proper.

7. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

8. During a telephone conversation with Anthony Murabito on 19 April 2005 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-7, 17-20. Affirmation of this election must be made by applicant in replying to this Office action. Claims 8-16, 21-25 withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1, 3, 5, 7, 17-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Saito, U.S. Patent No. 5,867,579. Referring to claims 1, 17, 20, Saito discloses a data copyright management system wherein the system comprises a primary user terminal and a copyright management center with database (Col. 3, lines 55-60 & Fig. 1), which meets the limitation of a first logical circuit having a local processor and local memory and a second logical circuit respectively. A user at the primary user terminal uses the system to request access to data by generating a public key (Col. 4, lines 20-21), which meets the limitation of generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit. The database of the copyright management center generates a secret key (Col. 4, line 33), which meets the limitation of determining a first decryption key for said encrypted signal at said second logical circuit. The data is encrypted and sent to the user terminal (Col. 12, lines 41-63), which meets the limitation of the second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit. When the user selects data that the user wishes to access, the user transmits the public key to the copyright management center/database and the copyright management center/database encrypts the secret key with the public key (Col. 4, line 42-67), which meets the limitation of encrypting the first decryption key at said second logical circuit by use of said public encryption key. The requested data is transmitted to the user in encrypted form (Col. 5, line 12), which meets the limitation of accessing an encrypted signal at said first logical circuit. The encrypted secret key is transmitted to the user (Col. 5, lines 13-14), which meets the limitation of transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link. The user then decrypts the encrypted secret key with the user's private key (Col. 5, lines 23-

25), which meets the limitation of at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key. The user then uses the decrypted secret key to decrypt the encrypted requested data (Col. 5, lines 39-42), which meets the limitation of at said first logical circuit, decrypting said encrypted signal using said first decryption key.

Referring to claim 3, Saito discloses that the public key of the user is stored in a first area of local memory at the copyright management center (Col. 12, lines 21-22), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The encryption program is stored in a different area of local memory at the copyright management center (Col. 11, lines 21-25), which meets the limitation of accessing a computer control program from a second portion of local memory at said second logical circuit, and executing said computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

Referring to claims 5, 18, 19, Saito discloses the user then decrypts the encrypted secret key with the user's private key (Col. 5, lines 23-25) using an copyright management program (Col. 5, line 5), which meets the limitations of accessing a second decryption key from a first portion of local memory at said first logical circuit, accessing a computer control program from a second portion of local memory at said first logical circuit, and executing said computer control program to decrypt said first decryption key using said second decryption key, a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical

circuit, modifiable local memory enabling the modification of a computer control program stored within said local memory.

Referring to claim 7, Saito discloses that the data is compliant with the MPEG format (Col. 1, line 48).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Saito, U.S. Patent No. 5,867,579, in view of Schneier. Referring to claim 2, Saito discloses uses public key cryptography (Col. 3, lines 12-24) but does not use the Diffie-Hellman algorithm for key exchange. Schneier discloses using the Diffie-Hellman algorithm for public key exchange (Pages 513-514). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in the data copyright

management system of Saito because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

14. Claims 4, 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito, U.S. Patent No. 5,867,579, in view of Yagawa, U.S. Patent No. 6,751,598. Referring to claims 4, 6, Saito discloses that the public key of the user is stored in a first area of local memory at the copyright management center (Col. 12, lines 21-22), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The encryption program is stored in a different area of local memory at the copyright management center (Col. 11, lines 21-25), which meets the limitation of accessing a computer control program from a second portion of local memory at said second logical circuit, and executing said computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key. Saito discloses the user then decrypts the encrypted secret key with the user's private key (Col. 5, lines 23-25) using an copyright management program (Col. 5, line 5), which meets the limitations of accessing a second decryption key from a first portion of local memory at said first logical circuit, accessing a computer control program from a second portion of local memory at said first logical circuit, and executing said computer control program to decrypt said first decryption key using said second decryption key. Saito does not disclose that the encryption program or the copyright management program is updated/replaced. Yagawa discloses a digital content distribution system wherein the system provides downloadable updates of the digital content (Col. 2, lines 16-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to upgrade/replace the encryption program and

Art Unit: 2132

the copyright management program of Saito in order to provide the user with the latest edition of programs as taught in Yagawa (Col. 4, lines 64-67).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON, JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100